Traducción del artículo:

# CIFRADO Y DESCIFRADO: Comunicar con toda seguridad.

De Autor Jean-Luis Nicolás.
Por Lucía Contreras Caballero.

*En el mundo actual, en el que las telecomunicaciones ocupan un sitio crucial, la criptografía es una apuesta mayor. Ha llegado a ser una ciencia compleja, que no puede pasar sin matemáticas de alto nivel.*

En marzo del 2000, un gran titular era común a todos los periódicos: “Alerta a la seguridad de las tarjetas de banco”¿Qué había pasado? En Francia, el secreto de las tarjetas manuales estaba protegido desde 1985 gracias a un método de cifrado en el que toma parte un gran número N, que consta de 97 cifras. Este número N debe ser producto de dos números primos grandes, es decir, de números que, como 7 o 19 no son divisibles más que por 1 y por ellos mismos. El secreto de una tarjeta de banco está constituido precisamente por esta pareja de números primos; calcularlos partiendo de N era prácticamente imposible en los años 80. Pero con el aumento de la potencia de los ordenadores y la mejora de los métodos matemáticos, el tamaño de los números N de los que se puede calcular los factores primos en un tiempo razonable ha sobrepasado la centena de cifras en los últimos años del siglo XX (el

récord en la fecha de enero de 2002 estaba en 158 cifras). Un informático astuto, Serge Humpich, pudo encontrar los dos números primos ultrasecretos de los que el producto valía N y los había utilizado para hacer tarjetas falsas. Entonces, para garantizar la seguridad de nuestros rectangulitos de plástico, el organismo de gestión de las tarjetas de banco ha construido enseguida nuevos números N claramente más grandes.

*La criptografía moderna, en el crecimiento de las matemáticas y de la informática.*

Esta peripecia ilustra la importancia considerable que tiene hoy día la ciencia del cifrado, es decir de la codificación de los mensajes con el propósito de hacerlos ilegibles a personas indiscretas. Cifrar y descifrar mensajes es una vieja actividad de varios siglos, pensar en milenios. Y esta actividad ha desbordado ampliamente el cuadro estrictamente militar o diplomático para ser otorgado a paneles enteros del universo de comunicaciones civiles: procesos de autentificación , transacciones entre bancos, comercio electrónico, protección de zonas y ficheros informáticos, etc.

La criptografía ha tenido muchos avances en las últimas décadas. Al hacerlo se ha hecho una ciencia compleja, donde los progresos son generalmente el hecho de que los especialistas han recibido una fuerte formación en matemáticas y en informática. Esta especialización se ha manifestado desde la segunda guerra mundial. Se conoce hoy el descifrado por los aliados de los mensajes codificados por las famosas máquinas alemanas. Ahora bien, es un eminente matemático británico, Alain Turing,

también uno de los padres de la informática teórica, quien ha aportado una contribución esencial a este descifrado.

En los años 70, la criptografía ha conocido una pequeña revolución: la invención de la criptografía con “llave pública” con el método RSA. ¿De qué se trata? Los interlocutores que querían intercambiar mensajes secretos debían compartir una llave secreta y el riesgo de ser averiguada esta llave por el enemigo era grande. El protocolo RSA, llamado así por sus tres inventores (Ronald Rivest, Adi Shamir y Leonard Adlman) resolvió el problema. Este método utiliza dos llaves: una llave de cifrado público—puede ser conocida por todos—y una llave de descifrado, que sigue siendo secreta. Esta está basada en el principio de que es posible construir grandes números primos (de cien, mil cifras o más) pero que es extremadamente difícil volver a encontrar los factores primos p y q de un número grande N=pxq. Esquemáticamente, el conocimiento de N depende del de la llave pública de cifrado, mientras que el conocimiento de p y q depende del de la llave secreta de descifrado.

Evidentemente, si alguien encontrara un método para descomponer rápidamente en sus factores primos, números grandes, el protocolo RSA caducaría. Pero también podría ser que los matemáticos probaran que tal método no existe, lo que reforzaría la seguridad del protocolo RSA. Estos son temas decisivos de investigación.

Los métodos que, como el protocolo RSA, hacen intervenir la teoría de números elaborada, dan una gran lección: Investigaciones matemáticas (sobre los números primos especialmente) completamente desinteresadas

pueden revelarse, años o décadas más tarde cruciales para tal o tal aplicación; y esto de manera imprevisible. En su libro *apología de un matemático* el gran teórico británico G. H. Hardy (1877—1947), que era un ferviente pacifista se enorgullecía de trabajar en un dominio perfectamente puro, la aritmética, y de no haber hecho nada que pudiera ser considerado útil. Sus trabajos eran, quizá, inútiles en su época. Hoy es falso.

*Curvas elípticas: la geometría algebraica al servicio de los comisionistas secretos.*

Y ello no concierne únicamente la teoría de números. Otros dominios de las matemáticas, antes consideradas desprovistas de aplicaciones, contribuyen a la ciencia de la criptografía. Métodos criptográficos prometedores y basados en principios similares de los del protocolo RSA han aparecido en los últimos años. Ocurre con el método llamado del logaritmo discreto. Lo que ha servido al mismo tiempo a concebir métodos que se apoyan en las propiedades de las curvas elípticas. No se tratan de curvas que tengan las propiedades de una elipse, sino de curvas cuyo estudio empezó en el siglo XIX para resolver el difícil problema del cálculo de la medida de una elipse. Estas curvas de ecuación  una expresión donde el cuadrado de *y* es igual a un polinomio sin segundo grado en *x*, con monomio principal el tercer grado en *x*,  tienen interesantes propiedades—cuyo estudio forma parte de la geometría algebraica, vasto dominio de las matemáticas actuales. Por ejemplo, con la ayuda de una construcción geométrica apropiada es posible definir una suma entre los puntos de una curva elíptica. Más generalmente, los objetos geométricos llamados curvas elípticas poseen

propiedades aritméticas—que se continua investigando—susceptibles de servir a la criptografía. Es así como ha sido desarrollado un método criptográfico que se llama *logaritmo discreto sobre curvas elípticas*

Otra dirección de investigación se ha revelado recientemente. En el congreso internacional de matemáticas de Berlin en 1988, Peter Shor, de los laboratorios AT&T, obtenía el premio Nevanlinna por sus trabajos sobre la criptografía cuántica. ¿Qué significa este término? Hace algunos años que físicos y matemáticos han imaginado que un día sería posible realizar un ordenador cuántico, es decir, cuyo funcionamiento empleara las extrañas leyes de la física cuántica, las que reinan el mundo de lo infinitamente pequeño. Ahora bien, uno se da cuenta de que tal ordenador, de ser realizable, sería capaz de factorizar muy rápidamente y haría así ineficaz el método RSA. Por otra parte, investigaciones hacia la realización concreta de un ordenador cuántico han sido publicadas muy recientemente, en la revista británica Nature. (referencia a final). Por otro lado, investigadores han elaborado protocolos de criptografía cuántica, es decir, métodos de cifrado utilizando objetos (fotones, átomos,…) que obedecen las leyes cuánticas. Estos protocolos cuánticos podrían una seguridad infalible. Todo ello está siendo estudiado y es posible que se haga operacional en algunos años.

Jean Louis Nicolas.
Institut Girard Desargues, Mathématiques.
Université Claude-Bernard (Lyon 1).

Algunas Referencias.

D. Kahn, Lagurre des codes secrets  (Intereditions, 1980).

J. Stern, La science du secret. (Odile Jacob, 1998.

S. Sing, Histoire des codes secrets (J.C. Lattès, 1999)

J. P. Delahaye, Merveilleux nombres premiers (Belin /Pour la Science).

D. Stinson, Cryptographie, théorie et pratique (Vuibert,2001).

L.M.K. Vandersypen et al. ”Experimental realization of Shork quantum factoring algorithm using nuclear magnetic resonance”, Nature vol 414. pp. 883-887 (20 décembre 2001).